

*The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.*

**TLP: WHITE**

**Disclosure is not limited. Subject to standard copyright rules, TLP: WHITE information may be distributed without restriction.**

<http://www.us-cert.gov/tlp/>

**DATE(S) ISSUED:**

09/25/2019

**SUBJECT:**

Multiple Vulnerabilities in Adobe ColdFusion Could Allow for Arbitrary Code Execution (APSB19-47)

**OVERVIEW:**

Multiple vulnerabilities have been discovered in Adobe ColdFusion, the most severe of which could allow for arbitrary code execution. Adobe ColdFusion is a rapid web-application development platform used to create and maintain web applications. Successful exploitation of the most severe of these vulnerabilities could result in an attacker executing arbitrary code in the context of the affected application. Depending on the privileges associated with this application, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. If this application has been configured to have fewer user rights on the system, exploitation of this vulnerability could have less impact than if it was configured with administrative rights.

**THREAT INTELLIGENCE:**

There are no reports of these vulnerabilities being exploited in the wild.

**SYSTEMS AFFECTED:**

- Adobe ColdFusion 2018 update 4 and earlier
- Adobe ColdFusion 2016 update 11 and earlier

**RISK:**

**Government:**

- Large and medium government entities: **High**
- Small government entities: **Medium**

**Businesses:**

- Large and medium business entities: **High**
- Small business entities: **Medium**

**Home users: Low**

**TECHNICAL SUMMARY:**

Multiple vulnerabilities have been discovered in Adobe ColdFusion, the most severe of which could allow for arbitrary code execution. Details of these vulnerabilities are included below:

- A Security bypass vulnerability that could allow for Information Disclosure. (CVE-2019-8072)

- A Command Injection via Vulnerable component that could allow for Arbitrary Code Execution. (CVE-2019-8073)
- A Path Traversal vulnerability that could allow for Access Control Bypass. (CVE-2019-8074)

**NOTE: Additional JEE, Java Enterprise Edition, and JDK, Java Development Kit, requirements must be met in addition to applying patches.**

Successful exploitation of the most severe of these vulnerabilities could result in an attacker executing arbitrary code in the context of the affected application. Depending on the privileges associated with this application, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. If this application has been configured to have fewer user rights on the system, exploitation of this vulnerability could have less impact than if it was configured with administrative rights.

#### **RECOMMENDATIONS:**

The following actions should be taken:

- Install the updates provided by Adobe immediately after appropriate testing.
- Ensure JDK, Java Development Kit, and JEE, Java Enterprise Edition, requirements and/or configuration changes are met after applying patches.
- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.
- Remind users not to visit websites or follow links provided by unknown or untrusted sources.
- Inform and educate users regarding the threats posed by hypertext links contained in emails or attachments especially from un-trusted sources.
- Apply the Principle of Least Privilege to all systems and services.

#### **REFERENCES:**

##### **Adobe:**

<https://helpx.adobe.com/security/products/coldfusion/apsb19-47.html>

##### **CVE:**

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=2019-8072>

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=2019-8073>

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=2019-8074>

#### **TLP: WHITE**

**Disclosure is not limited. Subject to standard copyright rules, TLP: WHITE information may be distributed without restriction.**

<http://www.us-cert.gov/tlp/>

This message and attachments may contain confidential information. If it appears that this message was sent to you by mistake, any retention, dissemination, distribution or copying of this message and attachments is strictly prohibited. Please notify the sender immediately and permanently delete the message and any attachments.

**Chris Watts**

Security Operations Analyst

MS Department of Information Technology Services

601-432-8201 | [www.its.ms.gov](http://www.its.ms.gov)



DISCLAIMER: This email and any files transmitted with it are confidential and intended solely for the use of the individual or entity to whom they are addressed. If you have received this email in error please notify the system manager. This message contains confidential information and is intended only for the individual named. If you are not the named addressee you should not disseminate, distribute or copy this e-mail. Please notify the sender immediately by e-mail if you have received this e-mail by mistake and delete this e-mail from your system. If you are not the intended recipient you are notified that disclosing, copying, distributing or taking any action in reliance on the contents of this information is strictly prohibited